AMENDMENTS TO THE CLAIMS

A detailed listing of all claims that are, or were, in the present application, irrespective of whether the claim(s) remains under examination in the application are presented below. The claims are presented in ascending order and each includes one status identifier. Those claims not cancelled or withdrawn but amended by the current amendment utilize the following notations for amendment: 1. deleted matter is shown by strikethrough; and 2. added matter is shown by underlining.

1.-24. (Cancelled)

25. (New) A method for initiating a private secure connection between at least one client and a remote server for transmission of enciphered communications over a public network using a layered communications protocol characterized by a protocol stack, the method comprising the steps of:

providing a first secure receipt pre-processor equipped to run a first process to enable communications with the at least one client;

communicatively coupling a first response manager to the first secure receipt pre-processor;

placing the remote server in data communications with the first secure receipt pre-processor and the first response manager, the data communications being intermediated by the protocol stack and the remote server being configured with an operating system operative to selectively direct a first secure server process;

receiving at the first secure receipt pre-processor a first client request originating at the at least one client and expressing at least one client capability supporting the initiation of the private secure connection with the remote server;

responsive to the receipt of the first client request, generating at the first secure receipt pre-processor, under control of the first process, a portion of a complete response to the client that is consistent with the at least one capability expressed in the first client request;

based upon the portion of the complete response and the layered communications protocol, generating at the response manager and communicating to the at least one client the complete response responsive to the first client request and expressing at least one server capability for supporting the initiation of the private secure connection with the at least first client;

responsive to the receipt of the complete response at the client, receiving at the first secure receipt pre-processor a first client reply containing a pre-master secret transmitted from the client, the pre-master secret being based at least in part upon the complete response communicated to the client by the response manager;

responsive to the first client reply, creating a first remote server response under direction of the first secure server process by using the first client request forwarded to the remote server through the intermediation of the protocol stack;

communicating the first remote server response to the response manager, through the intermediation of the protocol stack to cause the response manager to communicate the client reply, through the intermediation of the protocol stack, to the remote server;

under direction of the first secure server process, generating a session key using the pre-master secret in the client reply; and

encrypting communications, intermediated by the protocol stack, between the remote server and the at least one client over the public network using the session key.

26. (New) A method for initiating a private secure session for secured data communications over an unsecured network, the method comprising:

providing a server running under an operating system that controls at least a first process and a second process, the server including a secure receipt pre-processor, a response manager and a secure processor communicatively coupled to each other, wherein the secure receipt pre-processor and optionally the response manager are operationally directed by the first process and the secure processor is operationally directed by the second process;

receiving a first client hello from a client at the secure receipt pre-processor, the client hello including at least one first expression indicative of initiating the private secure session with the secure processor;

buffering the first client hello at the secure receipt pre-processor after assigning a secure session identifier to the first client hello;

responsive to the first client hello, generating a first server hello cooperatively between the secure receipt pre-processor and the response manager independent of the second process, the server hello including at least one second expression to enable the client to initiate the private secure session;

receiving a first client reply at the secure receipt pre-processor responsive to the first client hello, the first client reply being in a first ciphertext form and including at least one pre-master secret based at least in part on the at least one second expression;

responsive to receiving the first client reply, forwarding the first client hello, that matches client reply that corresponds to the buffered dial hello at the secure receipt pre-processor, to the secure processor to cause the secure processor to register the secure session identifier associated with the first client hello with the private secure session;

using the pre-master secret in the first client reply to generate a session key at the secure server; and

encrypting communications between the client and the secure server using the session key.